Met de kennis van nu, en met de rechtswetenschap als bril:* enkele gedachten over de Cyberpest

College van 26 maart 2010 ter gelegenheid van het afscheid van

Aernout Schmidt als gewoon hoogleraar recht en informatica†

*Eerbiedig ontleend aan August Willemsen [Willemsen(1987)].

†Mr. Aernout Schmidt is hoogleraar Recht en Informatica aan de Universiteit Leiden (bij eLaw@Leiden, Centrum voor recht in de informatiemaatschappij). Hij specialiseert zich in (methoden en technieken voor) de kwalitatieve analyse van (voorgenomen) regelstelsels voor institutionele systemen, die worden ondersteund door ICT. Zijn aandacht gaat daarbij uit naar (juridische aspecten van) functionele specificaties bij aanbesteding (zie bijvoorbeeld: [Schmidt and Corvers(2009)]). Hij is bestuurslid van de stichting Recht & Informatica Leiden en van de stichting Eupian (een Europees netwerk van commerciële en wetenschappelijke partners, gericht op het bevorderen van kennis over de mogelijke relaties tussen aanbesteding en innovatie). Hij heeft via Eupian een relatie met Corvers Procurement Services BV en is vaste adviseur van Croon Davidovich advocaten te Amsterdam. Hij neemt op 27 maart 2010 afscheid als gewoon- en treedt op 1 april van dat jaar in deeltijd (0.2 fte) aan als onbezoldigd hoogleraar Recht en Informatica.

Contents

1 Intro

Waarin ik mijn wetenschappelijke basishouding schets en de grote lijn[1] *aangeef*

Ik begin met een halve vergelijking. Hij is afkomstig van Oliver Wendell Holmes Jr. die hem rond 1900 bij een tafelrede gebruikte.[2] Hij luidt (in mijn vertaling) als volgt:

"Zoals de rups een cocon spint voor het gevleugelde wezen dat hij nooit zag maar desalniettemin worden zal, zo ..."

Korter dan via dit geleende beeld kan ik u geen indruk geven van mijn wetenschappelijke basishoudig. Alles wat leeft neemt maatregelen om zich en zijn soort te doen voortbestaan. Die maatregelen moeten evenwel worden genomen met onvolledige kennis: individuen handelen ook zonder dat zij de effecten ervan op zichzelf, op hun gemeenschap en op de omgeving volledig kunnen doorzien, net zomin als zij de invloed van hun omgeving op hun handelen volledig kunnen doorzien. Voor een rups is de beschikbare kennis voornamelijk opgeslagen in zijn DNA. Voor de mens komt daar zijn cultuur bij – en zowel de wetenschapsbeoefening als het recht zijn daarvan onderdelen.

Deze basishouding leidt tot het besef dat na verloop van tijd alles eruit gaat zien alsof het een functie heeft of had. Het Franse vestingdorp *was* er om de vijand te weren, *werd* later in zijn groei beperkt door zijn eigen muren

en *is* er anno 2010 nog steeds, maar nu om toeristen te behagen. Voor de wetenschap is het dan de kunst om één en ander in zijn context te beschrijven en te verklaren, en om functies van oorzaken te scheiden.[3]

Dit perspectief is mijn vertrekpunt.[4] Wat volgt gebruik ik om de halve vergelijking te betrekken op mijn vakgebied, informatietechnologie en recht, en om hem af te maken.

Ik begin met de aankondiging van een vooralsnog denkbeeldige ramp en eindig met enkele overwegingen over of de rechtswetenschap heeft bijgedragen aan het ontstaan van die dreiging en of hij kan bijdragen aan het beteugelen ervan.

2 Een casuspositie

Waarin de fictieve casus wordt geschetst als conceptuele basis van de Cyberpestdreiging

Ik leg u een fictieve casus voor.

Een maand geleden werd ik gebeld. Ik nam op en werd door een bandopname uitgenodigd om toets 1 te toetsen. Stel dat ik dat deed en dat me vervolgens door diezelfde bandopname gevraagd was een moment geduld te hebben. En stel dat gedurende de periode dat ik wachtte op de één of andere geheimzinnige wijze mijn mobiele telefoon vanuit Cyberspace is *gehackt*, en wel zodanig, dat hij daarna benut kan worden om, na een teken van buiten, SMS-berichten te zenden aan vijf geselecteerde telefoonnummers uit mijn adreslijst. En stel bovendien, dat op een vergelijkbare geheimzinnige wijze een weerzinwekkend filmpje met kinderpornografische inhoud in het geheugen van mijn telefoon is geplaatst en vervolgens is doorgezonden naar de e-mailadressen van diezelfde personen, ditmaal aangevuld met een misdaadverslaggever – dit alles zonder dat ik dat zelf merk en op een wijze die geen sporen van de *hack* achterlaat op mijn Blackberry. Misschien is het goed om deze vooralsnog fictieve gebeurtenis even te laten inwerken.[5]

Hoe zou *u* zich voelen in mijn plaats, wanneer *'uw'* gedrag in de krant aan de kaak is gesteld en *u* door een voorin-

genomen Officier van Justitie na *uw* aanhouding aan de tand wordt gevoeld?

Of – erger nog – hoe zou Balkenende zich voelen wanneer dit hem overkwam, één maand vóór de verkiezingen?

Of – wellicht nog erger – hoe zouden *wij* ons voelen wanneer dit soort *hacking* op zeer grote schaal zou voorkomen? En hoe zou de maatschappelijke chaos eruit zien die daar het gevolg van zou zijn?

3 Cyberpest en rechtsbescherming

Waarin de individuele rechtsbescherming tegen de Cyberpest wordt besproken en het begrip 'Cyberpest' wordt geïntroduceerd

Laten we eens bezien welke rol is weggelegd voor het recht als instrument van rechtsbescherming voor het slachtoffer. Ik bespreek die rol bij het beschreven drama, maar dan zoals zich dat zou hebben kunnen afspelen op de denkbeeldige Blackberry van Balkenende omdat we dan vermoedelijk beter bij de les blijven.

In Nederland is alleen al het beschikbaar hebben van kinderpornografisch materiaal strafbaar. Het verspreiden ervan is dat ook en wordt doorgaans zwaarder gestraft. De maximumstraf is voor beide delicten onlangs verhoogd tot 8 jaar. Ik ga ervan uit dat zowel het beschikbaar hebben op de Blackberry als het verspreiden via de Blackberry kan worden bewezen op basis van bewaarde telecommunicatieverkeersgegevens. Omdat er geen precedenten zijn waarin de lijsttrekker van een belangrijke politieke partij verdachte is geweest moet ik afgaan op wat de doorsnee kinderpornobezitter overkomt: een aanmerkelijke taakstraf of een bescheiden vrijheidsstraf. Op het eerste gezicht staat Balkenende er niet best voor.

Even tussendoor: in het vervolg zal ik de term *agent* regelmatig gebruiken. Ik bedoel dan computertjes of pro-

gramma's die zelfstandig handelen. Balkenende's Blackberry is zo'n *agent*, en Cyberspace zit er vol mee.[6]

Terug naar de casus. Wanneer we het relevante positieve recht nader beschouwen dringen de volgende twee vragen zich op: kan de wet zo worden gelezen dat mag worden aangenomen

- dat wat *de Blackberry* van Balkenende deed *door Balkenende zelf* is gedaan

en, zo ja, kan dan worden aangenomen

- dat wat *de Blackberry* van Balkenende deed *opzettelijk* door Balkenende is gedaan.

Wanneer geen sporen van een *hack* kunnen worden gevonden en ook geen ander overtuigend tegenbewijs wordt gegeven, wordt als bewezen aangenomen dat wat de Blackberry van Balkenende deed *opzettelijk door Balkenende is gedaan.* Dit is vaste rechtspraak die ertoe leidt dat het zogenoemde '*hacker*-verweer' maar zelden gehoor vindt. Ook door een positiefrechtelijke bril zit Balkenende in de puree.

Dit is sneu. Balkenende *weet* domweg dat wat zijn Blackberry heeft gedaan niet door hemzelf is gedaan, en zeker niet opzettelijk. Hij weet niet hoe dat-wat-gebeurd-is

heeft kúnnen gebeuren, maar *hij* was het niet. Hij weet dat het OM en de rechter dat-wat-echt-gebeurd-is ook niet weten. Intussen ziet hij *wél* zijn carrière door de goot wegspoelen – de Nieuwe Revu heeft er lucht van gekregen en erover gepubliceerd met beschadigende beeldcitaten. Pauw en Witteman bespreken meesmuilend de mogelijkheid dat hij onschuldig is en laten doorschemeren dat hij *hén* nog meer kan vertellen. Hoogleraren informatica passeren in de media de revue en zeggen allemaal wat anders. Maxime Verhagen staat niet alleen klaar om het lijsttrekkerschap over te nemen zodra *hij, Balkenende,* het neerlegt, maar slaagt er bovendien in de suggestie te wekken dat Cohen achter de affaire zit. Davids zegt onvoldoende van de casus te weten om een opinie te kunnen geven, laat staan een rechtswetenschappelijk oordeel. Het zou mij niet verbazen wanneer Balkenende onder deze omstandigheden een deel van zijn vertrouwen in de Nederlandse rechtsorde verliest, omdat die hem niet beschermt, maar veroordeelt.

Beschermt waartegen? Tegen twee dingen:

- ten eerste tegen het ten onrechte door een rechter verantwoordelijk worden gehouden voor gedrag van *agents* die niet naar de instructies van hem, Balkenende handelden

en

- ten tweede bescherming tegen het verlies van vertrouwen in de rechtsorde dat zou ontstaan wanneer zulks op grote schaal zou gebeuren. En *dat* dit op grote schaal kan gebeuren zal ik straks laten zien als ik iets zeg over *root kits, botnets* en *bounds checks.* Voorlopig nodig ik u uit om ook zonder nadere onderbouwing met mij mee te denken en deze dreiging als een *reële* dreiging te aanvaarden.

Ik geef u, om één en ander toch alvast een beetje aannemelijk te maken het bericht dat Microsoft mij en vele anderen op 9 maart jongstleden zond als toelichting bij een "critical update" van MS-Office (in mijn vertaling):

> *"Deze update bevat verschillende verbeteringen om de stabiliteit en de werking te verbeteren. Hij bevat tevens verbeteringen voor kwetsbaarheden die een aanvaller gebruiken kan om de inhoud van het geheugen van uw computer te overschrijven met kwaadaardige programmatuur."*

De aanhef van dit bericht klinkt bemoedigend maar verhult niet dat de meest populaire tekstverwerker ter wereld op 9 maart jongstleden nog kwetsbaarheden bevatte die kwaadwillende *agents* toestonden om de controle over mijn en uw computer over te nemen (en over de computers van alle andere gebruikers van die tekstverwerker) en er kinderporno in te plaatsen - ik noem maar een voorbeeld.

Als gezegd ontvangen we dit soort berichten met *critical updates* om de haverklap van *alle* belangrijke softwareproducenten. We hebben een situatie laten ontstaan die zich laat vergelijken met wat voorafging aan de kredietcrisis: we hebben ons op grote schaal afhankelijk gemaakt van ondoorzichtige producten van dubieuze kwaliteit, met alle risico's van dien – risico's die tegenwoordig ook wel systeemrisico's worden genoemd. En ik durf de stelling wel aan dat een *serieuze, goedgeorganiseerde aanval* aanmerkelijk sterkere repercussies hebben *kan* dan de kredietcrisis zoals we die tot nu toe kennen. Tenslotte zal de financiële sector er *zelf* ook het slachtoffer van zijn.

Deze dreiging noem ik verder de dreiging van de *Cyberpest*, als aanduiding voor een besmettelijke aandoening die onze hele maatschappelijke orde kan aantasten. Een belangrijke eigenschap van de Cyberpest is dat hij op het moment van toeslaan de bewijzen van zijn eigen oorzaken en werking verloren doet gaan of anderszins verbergt.

Ik vat samen in twee stellingen:

Met de kennis van nu ondervinden slachtoffers van Cyberpestaanvallen nauwelijks rechtsbescherming van het positieve recht.

Onmiddellijk in samenhang hiermee is mijn tweede stelling:

Met de kennis van nu kunnen kwaadwillenden in de informatiemaatschappij een Cyberpestepidemie veroorzaken zonder veel risico te worden opgespoord en vervolgd.

4 Cyberpest als systeemdreiging

Waarin de Cyberpestdreiging als systeemdreiging wordt geïntroduceerd

Het Cyberpestrisico lijkt ook in een ander opzicht op wat de kredietcrisis heeft laten zien: wie ondoorzichtige financiële producten koopt zit niet alléén in het schuitje dat de resulterende maatschappelijke storm moet doorstaan, wie ze niet kocht vaart toch mee. Wie ondoorzichtige ICT-producten koopt is niet de enige die zal moeten leven in de erop volgende Cyberpestchaos, dat moeten we allemaal.

Mede daarom denken we over onze rechtsorde niet alleen als instrument voor individuele rechtsbescherming maar ook als een patroon dat zich ontwikkelt gedurende de tijd, een patroon dat we zelf maken en dat aan onze *maatschappelijke* orde stabiliteit kan bezorgen, ook in tijden waarin de omstandigheden zodanig wijzigen dat aanpassingen noodzakelijk zijn.

We zijn met dat laatste beeld vertrouwd. We herkennen het in de rol die we het recht toekennen bij zo uiteenlopende bedreigingen als – ik noem slechts twee andere voorbeelden – de opwarming van de aarde en de ineenstorting van de financiële sector. Ik geef een paar overeenkomsten

met de Cyberpestdreiging:

- Ook op die bedreigingen lijkt het positieve recht geen vat te hebben.
- Ook bij die bedreigingen verwachten we dat het recht of aanpassingen ervan ertoe zullen bijdragen ze effectief tegemoet te treden.
- Ook bij die bedreigingen gaat het om grensoverschrijdende belangen waarop ons internationale publiekrecht maar geen werkelijke greep op lijkt te krijgen.
- Ook bij die bedreigingen zijn het de regelmatigheden in menselijk gedrag die ertoe leiden dat de omgeving zozeer verandert dat *onze rechtsorde* er niet veel langer of maar heel moeizaam in zal kunnen overleven.

Deze vier overeenkomsten geven aan dat er bij de Cyberpestdreiging – net als bij de kredietcrisis en bij de opwarming van de aarde – sprake is van wat tegenwoordig wel een systeemdreiging wordt genoemd.

In termen van systeemdreigingen heeft de maatschappelijke orde een deels hiërarchische en deels spaghetti-achtige structuur die is opgebouwd uit hele collecties van regelgeleide gemeenschappen welke door actoren worden gevormd en in stand gehouden. Ik acht het bijzonder aannemelijk dat het vormen en overleven van regelgeleide ge-

meenschappen een proces is dat zinvol kan worden begrepen als een evolutionair proces dat deels wordt ontworpen door de deelnemende actoren en deels het 'blinde' resultaat is van wat de cultuur en de natuur aan de deelnemende actoren ingeeft om te doen tegen de voorliggende interne en externe bedreigingen, bedreigingen die ze doorgaans maar gedeeltelijk kunnen overzien.

5 Waar blijft de rechtswetenschap?

> *Waarin de vraag wordt aangesneden wat de rol van de rechtswetenschap ten aanzien van de Cyberpestdreiging is*

De vraag doet zich dan voor wat we bij de Cyberpest als systeemdreiging mogen verwachten van de rechtswetenschap. Mijn derde stelling geeft het antwoord:

Bij systeemdreigingen als de Cyberpest mogen we van de rechtswetenschap verwachten dat die eraan bijdraagt dat de noodzakelijke juridische en politieke keuzen zo *goed mogelijk geïnformeerd kunnen worden gemaakt – dat wil zeggen, met de kennis van nu.*

Ik moet u bekennen dat niet elke collega het op dit punt met mij eens is, vooral niet, wanneer ik probeer aan te geven dat wij – voorzover het gaat om de gevolgen voor de rechtsorde – de kennis uit andere disciplines mede in onze overwegingen moeten betrekken. Waar ieder het over eens is, is dat we eraan moeten bijdragen dat onze juridische uitspraken zodanig worden geformuleerd, dat de rechtsorde *intern* coherent blijft. *Mijn* stelling aanvaardt dat de rechtswetenschap ook een taak heeft waar het gaat om de *externe* coherentie van de rechtsorde waarover wordt nagedacht.

Het rechtswetenschappelijk zo goed mogelijk informeren

bij het onder ogen zien van kritische bedreigingen is helaas niet erg goed ontwikkeld. De rechtswetenschap pleegt traditioneel terug te kijken in de moraalgeschiedenis of omhoog naar de Allerhoogste(n), en een literaire benadering te verkiezen boven een empirische. Dat is, meen ik, de reden dat het empirische onderzoek naar valkuilen van deze soort door ons, juristen, in wetenschappelijke zin is prijsgegeven en – als vanzelfsprekend – door andere wetenschappen wordt veroverd. Ik denk dat we, hier en nu, veel meer kennis beschikbaar hebben die ons kan bijstaan de dreiging van een Cyberpestepidemie te domesticeren dan juristen zich plegen te realiseren. *Wij* komen zelden verder dan het verdedigen van opinies bij sprekende casusposities. (Ik denk dan bijvoorbeeld aan de *informer case* die Hart en Fuller nog verder uit elkaar dreef.)[7]

Maar inmiddels speuren ecologen, economen, sociologen en psychologen het bedoelde gebied theoretisch en empirisch af, en maken aanmerkelijke vorderingen – zowel inhoudelijk als methodisch.[8] Jammer genoeg blijken *zij* doorgaans even mager geïnformeerd over de resultaten van de rechtswetenschap als wij over hún resultaten. Dat de term *moral hazard* een bij uitstek economische term is zou ons in dit verband te denken kunnen geven.

Kortom: ik denk dat een Cyberpestepidemie een reële dreiging is. Ik denk ook dat de Cyberpestdreiging de externe coherentie van onze rechtsorde kan aantasten en om een multidisciplinaire aanpak vraagt, en dat daarbij

de analyse door een rechtswetenschappelijke bril niet kan worden gemist. Het ware wenselijk wanneer daarbij over en weer wordt geprofiteerd van de bevindingen van verschillende disciplines die hun eigen bril hebben opgezet en opgezet houden – ook wanneer ze de resultaten van elkaars werk op hun bruikbaarheid beoordelen.

Om op de betekenis hiervan bij de Cyberpestdreiging als systeemdeiging enig zicht te krijgen ga ik in het resterende deel van mijn betoog op zoek naar een antwoord op de vraag wat de rechtswetenschap zou kunnen bijdragen aan het domesticeren van de Cyberpestdreiging en hoe de rechtswetenschap daarbij niet-juridische wetenschapsresultaten kan gebruiken.

6 Met de informaticakennis van toen

Waarin de technische kant van de Cyberpest wordt geschetst

Misschien is het goed om dan eerst *door de bril van de informatica* iets te zeggen over de meest gangbare kwetsbaarheden die aan de werking van *agents* in Cyberspace kleven. *Agents* zijn kwetsbaar, of vertonen *vulnerabilities* zoals het spraakgebruik is geworden. Met name alle thans beschikbare systeemprogrammatuur (zoals MS-Windows, en de varianten van Linux en van Unix) vertonen ze. Er is een hele wapenwedloop ontstaan tussen wie die *vulnerabilities* willen misbruiken en wie de gaten willen dichten. Bij die wapenwedloop ligt het initiatief bij de kwaadwillenden. En aan hun kant, de kant die Hirshleifer als "the dark side of the force" aanduidt[9] is men vergaand gevorderd met het maken van wat *root kits* worden genoemd.

Dit zijn om het kort door de bocht te zeggen programma's die zich nestelen in de kernels van systeemprogrammatuur en die zich niet of nauwelijks laten opsporen. *Root kits* zijn kwartiermakers voor besturing op afstand, voor het uitvoeren van *malware* op commando. Ze zijn zo diep in uw systeem ingedrongen dat ze tot alles bevoegd zijn. Als uw systeem besmet is geraakt wordt het een 'bot' genoemd, omdat het zich vanuit uw gezichtspunt af en toe als een robot gedraagt en iets anders doet dan u verwacht.

Bots kunnen in netwerken samenwerken en hun doorgaans bedenkelijke activiteiten heel snel door het botnet van de één aan de ander overdragen. Ze worden er ook steeds behendiger in om de sporen van hun aanwezigheid te wissen en te verbergen. Kortom, ze zijn moeilijk te vinden en te verwijderen. Ze worden vooralsnog vooral gebruikt voor het verspreiden van *spam*, maar er zijn geen technische belemmeringen die hen zouden verhinderen om welk programma dan ook uit te voeren. Met het voortschrijden van de techniek – met name van die spectaculaire producten die tot de artificiële intelligentie worden gerekend – vind ik dat verontrustend.

Het Trendrapport 2009 van GovCert[10] geeft daar voeding aan. Het doet bijvoorbeeld verslag van het oprollen van het 'Sneker botnet,' dat meer dan 100.000 computers onder commando had. Niet door het op te sporen en te vernietigen, maar door een – vergeef me de uitdrukking – snotneus uit Sneek op te pakken toen die het wilde verkopen aan iemand die om andere redenen in de gaten werd gehouden.[11]

Een ironische indruk van de massale onzekerheid die een Cyberpestaanval kan veroorzaken volgde uit de manier waarop de KLPD het Sneker botnet heeft proberen te helpen opruimen: het zond een e-mailbericht aan de getroffenen waarin instructies over hoe de *root kit* kon worden verwijderd. Ik ben benieuwd hoe u zou reageren op een dergelijk bericht. Ik zou het vermoedelijk als gevaarlijk

hebben beschouwd en het niet eens hebben geopend.
Dit was het slechte nieuws. Nu over naar het goede.

7 Bounds checks

Waarin de technische remedie tegen de Cyberpest wordt geïntroduceerd

De beschreven kwetsbaarheden hadden kunnen worden vookómen. Het gaat om een betrekkelijk eenvoudige technische maatregel waaraan *agents* zich zouden moeten houden. We moeten ons daarbij realiseren dat de greep naar de macht door een *agent* over een andere *agent* alleen kan verlopen via code (dat wil zeggen via programmaonderdelen die worden uitgevoerd). Een goedwillend programma is gevoelig voor misbruik wanneer het data in een buffer kopiëert zonder te verifiëren of de weg te schrijven hoeveelheid past in de ruimte die is bestemd voor ontvangst. Wanneer over de grens van die ruimte wordt weggeschreven, kan informatie worden geïnjecteerd op een plaats die later gaat worden uitgevoerd als ware het een programma. Wanneer een kwaadwillende agent van deze eigenschap – die *buffer overflow vulnerability* wordt genoemd – gebruik maakt kan deze de zeggenschap over de goedwillende computer overnemen en een *root kit* installeren. Een eenvoudige en tegelijkertijd effectieve tegenmaatregel is om onmiddellijk voorafgaand aan het wegschrijven van data naar een buffer na te gaan of die informatie in de ervoor gereserveerde ruimte past. Die voorzorg wordt een *bounds check* genoemd.

Dit is geen nieuw idee: in zijn Turing Award Lecture van 1980 – dertig jaar geleden! – zei Hoare[12] er, in mijn vertaling, het volgende over:

> *In elke andere tak van techniek zou het niet in acht nemen van dergelijke elementaire voorzorgen al lang in strijd met het recht zijn geweest.*

Het is opmerkelijk dat de observatie van Hoare als een elementaire voorzorg tegen het maken van programmeerfouten is bedoeld, geformuleerd in een tijd dat het web er nog helemaal niet was. En dat die voorzorg, achteraf bezien ook bescherming zou hebben geboden tegen de belangrijkste internetkwetsbaarheden van nu.

Eén en ander neemt niet weg dat tot op de dag van vandaag de hierbedoelde elementaire zorgvuldigheid op grote schaal in de wind wordt geslagen bij het inrichten van programmatuur. En het enkele feit dat de marktleidende systeemprogrammatuur, database managementsystemen, *office suites* en *portable document format handlers* niet deze meest voor de hand liggende bescherming bieden dwingt ons onder ogen te zien dat wij, als gebruikers, er weinig anders aan kunnen doen dan een keuze maken: ofwel het deelnemen aan de informatiemaatschappij beëindigen, ofwel het risico aanvaarden. Bij de huidige stand van techniek kunnen we vaststellen dat de risico's bestaan en toenemen – ook waar het gaat om geregisseerd misbruik op

grote schaal – terwijl de lapmiddelen die thans in zwang raken geen aanvaardbare vorm van soulaas bieden.[13]

Ik vat opnieuw samen in een stelling:

Het in acht nemen van informaticakennis van vóór 1980 had de dreiging van de Cyberpest kunnen voorkomen.

We moeten ons dan afvragen of de rechtswetenschap van de waarschuwing van Hoare op de hoogte had moeten zijn en adequate maatregelen had moeten adviseren.

8 De rechtswetenschap als multifocale bril

Waarin twee focale gebieden van de rechtswetenschap worden ingezet

Stel nu, dat we onze beslissers, de rechters en de politici, door een rechtswetenschappelijke bril zo goed mogelijk willen informeren over de valkuilen die ze kunnen verwachten bij het inzetten van juridische middelen ter bestrijding van de Cyberpest. Ik moet dan eerst even waarschuwen dat de bril van de rechtswetenschap een multifocale bril is.[14] Er zijn twee afstanden[15] waarop kan worden scherp gesteld. Ik noem ze de twee provincies van de rechtswetenschap:

- De positivistische provincie, hier gaat het om de interpretatie van geldend recht in het licht van gedrag – dit is waar de rechtswetenschap zich onderscheidt van andere wetenschappen, waar zij excelleert en waar zij de interne coherentie van de rechtsorde mee helpt bewaken;
- De natuurrechtprovincie. Deze provincie van de rechtswetenschap is om veel redenen verdacht, maar komt steevast naar voren wanneer de rechtsorde zelf in moeilijkheden raakt. Ik vermoed dat de rechtswetenschap het scherpstellen op deze afstand zoveel moge-

lijk tracht te vermijden, hetgeen zou kunnen meebrengen dat we *er niet goed in zijn* en dat hier nog veel te leren valt. Maar dit is ook de provincie waar we een bijdrage kunnen leveren aan de bewaking van de externe coherentie van onze rechtsorde. De stellingname van Van Walsum in de Irak-discussie dat er omstandigheden kunnen zijn die rechtvaardigen om van het volkenrecht af te wijken hoort in deze provincie thuis, net zoals de tweede volzin van ons Plakkaat van Verlatinghe uit 1581 die het regime van Philips II als onaanvaardbaar afwijst. Ik denk dat we deze provincie van de rechtswetenschap in de informatiemaatschappij nogal eens nodig hebben en dat hij het beste kan worden omgedoopt. Het gaat dan om de rechtswetenschappelijke begeleiding van wat ik met een verwijzing naar Scheffer[16] kritische veranderingen van de maatschappelijke orde zou noemen. Reële, revolutionaire veranderingen dus, die ook vanuit de rechtswetenschap eerder om een empirisch-analytisch instrumentarium vragen dan om de metafysische aanpak die nu vooral in zwang lijkt te zijn. Inderdaad, ik doel op het fascinerende instrumentarium zoals dat wordt gebruikt door evolutionair georiënteerde ecologen, economen, sociologen en psychologen.

Ik nodig u nu uit om met mij door deze bifocale bril te kijken naar de Cyberpestdreiging.

Door de positivistisch geslepen lens ligt het voor de hand na te gaan of er mogelijkheden zijn geweest om iets meer te bereiken langs de lijnen van de gevaarzetting en/of zorgplicht uit het aansprakelijkheidsrecht, en naar de met de maatschappelijke ontwikkelingen meebewegende interpreties van begrippen als *de verkeersopvatting en de risico-aansprakelijkheid uit het civiele* recht, en het voorwaardelijk opzet uit het strafrecht. Uiteindelijk is de gedachte niet absurd dat het openzetten van een kelderluik of het marginaal markeren van een bussluis verwantschap vertonen met het verspreiden van systeemprogrammatuur die kwetsbaar is voor aanvallen van *agents* die *root kits* installeren via *buffer overflow vulnerabilities*. En ook kan men zich afvragen of het verspreiden van dergelijke producten niet kan worden gelijk gesteld met het welbewust nemen van een aanmerkelijk risico. Bij mijn weten is er evenwel geen rechtspraak die deze invalshoek omhelst. In de ICT-praktijk kan dan ook geen traditie worden ontwaard als in de auto-industrie. Wanneer een brandstoftank bij auto-ongelukken bovengemiddeld in brand vliegt of wanneer een gaspedaal een enkele keer blijft hangen wordt de autofabrikant voor eventueel volgende schade aangesproken en zorgt hij er voor om de oorzaken onmiddellijk weg te nemen. Maar wanneer systeemprogrammatuur infectie met Cyberpest toelaat is de schade voor rekening van het slachtoffer – de leverancier gaat in de praktijk doorgaans vrijuit en de veroorzaker is doorgaans onvindbaar.

Ik denk dat dit in beginsel anders kan en anders had ge-

kund – ook met het recht van nu. Ik vat dit op als een teken van kracht van ons positieve recht, al wordt aan dat teken afbreuk gedaan door gebrek aan toepassing. Maar dat is geen kwestie die door de focus van het positieve recht zichtbaar wordt.

Die kwestie wordt wél zichtbaar door de lens die zich richt op kritische veranderingen van de maatschappelijke orde. Daar is het *niet* gebruiken van positiefrechtelijke instrumenten een alarmsignaal op zichzelf. Alsdan moeten verklaringen worden gezocht, en moeten relevante verklaringen uit bijvoorbeeld de economie en de sociale wetenschappen niet worden geschuwd.

Het individuele slachtoffer van een *root kit* infectie, bijvoorbeeld, ondervindt doorgaans – zolang het doel zich beperkt tot het verzenden van *spam* – beperkte hinder of schade van die infectie, meestal merkt hij het niet eens. Dat inmiddels meer dan 90% van de bandbreedte die voor e-mails wordt gebruikt wordt geconsumeerd door *spam* leidt ook niet tot problemen die ergens anders als urgent worden ervaren. De gebruikte capaciteit wordt betaald via de abonnementen van de gebruikers, en de service providers die de capaciteit in- en verkopen zijn gebaat bij een zo hoog mogelijke omzet. Onze telecommunicatiewaakhond, de OPTA, zou aanmerkelijk meer en effectiever tegen *spam* kunnen optreden en daarmee tegen botnets, maar ziet andere kwesties kennelijk als dringender. Met andere woorden, en anders dan waar het gaat over het uit-

wisselen van door auteursrechten beschermd materiaal, er is eigenlijk niemand die het de moeite waard vindt om te investeren in toezicht of in het voorbereiden en doorzetten van individuele, relatief kleine en tegelijkertijd buitengewoon moeilijke en onzekere schadeclaims.

9 De evolutie naar kwetsbaarheid voor Cyberpest

Waarin het multidisciplinaire karakter van de rechtswetenschap – wanneer die wordt geconfronteerd met vragen die samenhangen met kritische veranderingen van de rechtsorde – nader wordt geïllustreerd

Laat ik nog een kort beeld schetsen over hoe de Cyberpestdeiging in onze informatiemaatschappij heeft kunnen postvatten aan de hand van enkele mijns inziens wél relevante, maar niet juridische inzichten die ik domweg in een lijstje opsom. Per inzicht noem ik een handvat voor rechtswetenschappelijke betekenisgeving.

1. Het eerste is sociaalwetenschappelijk van aard en roept het inzicht in herinnering dat wij, en met name regelgevers, de maakbaarheid der dingen plegen te overschatten.[17] Het is daarmee van belang voor de wetgever.

2. Het tweede komt uit de informatica en stelt dat een programmeur zich dient te houden aan de regels van structured programming, waartoe het uitvoeren van bounds check behoort.[18] Juridisch zou dit betekenis

kunnen hebben voor de interpretatie van wat we van een zorgvuldige en ter zake kundige programmeur mogen verwachten. Dit inzicht kan worden uitgebreid met een reeks verwante inzichten die ik hier niet noem omdat ze technisch van aard zijn.

3. Het derde inzicht komt uit de economie en zegt dat kennisasymmetrieën (zoals die plegen te bestaan tussen opdrachtgevers, makers en gebruikers van programmatuur) een gevaar kunnen opleveren voor het vertrouwen tussen partijen en zo een markt kunnen doen instorten.[19] De economie doet hier doorgaans een beroep op effectieve rechtsbescherming bij asymmetrische ad-hoc transacties.

4. Het vierde komt ook uit de economie en zegt dat kennisasymmetrieën (zoals die plegen te bestaan tussen opdrachtgevers, makers en gebruikers van programmatuur) ook een gevaar opleveren voor de overlevingskansen van een bedrijf of organisatie wanneer de benodigde kennis zo zeldzaam is dat er geen markt voor is, terwijl die kennis niet binnen het bedrijf kan worden belegd.[20] De economie doet hier opnieuw een beroep op effectieve rechtsbescherming, ditmaal bij asymmetrische duurcontracten.

5. Het vijfde inzicht komt opnieuw van de economen en zegt dat het prijsmechanisme van de markt niet goed werkt wanneer de voorwaarden daarvoor niet

zijn vervuld. De economie doet hier opnieuw een beroep op het recht, waar het recht die voorwaarden zou kunnen scheppen. Hierbij wordt meestal gedacht aan het mededingingsrecht.

Intussen is de markt met zijn prijsmechanisme in actie gekomen en zien we in de laatste jaren een ontwikkeling in de richting van intermediairs die ons vanuit een centrale plek beveiligde diensten aanbieden. *Softare as a Service* wordt dat genoemd. Meestal zijn aan het gebruik ervan beperkingen verbonden. Deze universiteit, bijvoorbeeld, maakt gebruik van Citrix en verbiedt de medewerkers om zelf software te installeren. De daaraan verbonden bezwaren worden door economen *moral hazards* genoemd.

6. Het zesde is opnieuw economisch van aard en waarschuwt tegen het ontstaan van een situatie waarin dienstverleners wel concurreren, maar daarbij gebruik blijven maken van een ingeburgerde vorm van marktfalen omdat ze er individueel geen baat bij hebben het algemene probleem aan te pakken. Bijvoorbeeld wanneer ze een bedrijfsmodel hebben dat afhankelijk is van het voortbestaan van de eerder beschreven vulnerabilities. Bij intermediairs is dat vaak het geval. Juridisch komen we hier opnieuw in de buurt van het mededingingsrecht maar ook hier lijkt de maatschappelijke werkelijkheid een evenwicht te hebben

gezocht dat een marktfalen inhoudt maar dat niet direct met het mededingingsrecht lijkt te kunnen worden aangepakt.

Er is een hele industrie ontstaan die er voordeel bij heeft dat de Cyberpestdreiging in stand blijft. Het is in dit verband misschien nuttig om als laatste nog een inzicht te noemen dat hierbij een rol kan spelen.

7. Het zevende inzicht is opnieuw economisch van aard en beveelt aan te voorkomen dat een situatie ontstaat waarin het bijzonder moeilijk is om een gekozen oplossing door een andere te vervangen. Economen spreken hier van *pad-afhankelijkheid*[21] die tot het vasthouden aan eenmaal gemaakte keuzen kan dwingen. Ook hier is voor het recht op het eerste gezicht weinig ruimte. Het probleem van pad-afhankelijkheid is, dat ook vanuit de vraagzijde de motivering ontbreekt om aanbieders naar andere en betere oplossingen te doen zoeken. Mogelijk kan hier bestuursrechtelijk een aanzet worden gegeven via het aanbestedingsrecht door de overheid, als grootafnemer, een inkoopbeleid te laten voeren dat het vermijden van pad-afhankelijkheden serieus neemt.[22]

Ik houd ermee op. Ik heb inmiddels 1 relevant inzicht uit de sociale wetenschap, 2 uit de informatica en 4 uit de economie genoemd en zou zo nog wel even kunnen door-

gaan. Ik heb voorts tegelijkertijd geprobeerd een eerste indruk te geven van hoe naar die externe inzichten kan worden gekeken door een rechtswetenschappelijke bril.

U begrijpt dat het vinden van een goedgefundeerd advies over hoe de Cyberpestdreiging met juridische middelen tegemoet kan worden getreden geen sinecure is.[23]

Er is nu geen tijd meer om verder te zoeken naar juridische oplossingen voor de Cyberpestdreiging, althans niet in dit college. Ik kan – concluderend – nog wel aangeven waar ik een uitweg verwacht. Eén van de belangrijkste stoorzenders voor een natuurlijke oplossing van veel problemen is het bestaan van kennisasymmetrieën tussen partijen die iets met elkaar moeten. Dit probleem treedt niet alleen op in de informatica tussen opdrachtgevers en makers. Het doet zich ook voor op de markt, en niet alleen die voor tweedehand auto's. Het treedt naar voren bij vrijwel elke aanbesteding. Het speelt ook wel eens in de rechtspraak. En het doet zich in wederkerige mate voor wanneer verschillende disciplines moeten samenwerken. De meest effectieve, algemene en goed-gefundeerde aanpak van het kennisasymmetrieprobleem zie ik in de methoden van requirements engineering die in de informaticadiscipline zijn ontwikkeld als antwoord op de software crisis van de jaren 70. Ik heb de laatste jaren gemerkt dat de werkwijze die daar voor het formuleren van stelsels van vereisten is ontstaan effectief kan worden vertaald naar een methode die zulke vereisten door een rechtswetenschappelijke bril for-

muleert. Ik heb ook gemerkt dat deze benadering vruchten draagt in de aanbestedingspraktijk, met name waar technische en functionele specificaties moeten worden beoordeeld. Corvers en ik publiceerden daar vorig jaar nog over.[24] Van der Klaauw en ik gebruiken die aanpak bij onze adviezen en Schmidt jr. zal er bij Croon Davidovich ook aan moeten geloven. Voorlopig zullen we er nog wel even werk aan hebben.

Intussen brengt het opschrijven van dit college me op de inmiddels voor de hand liggende gedachte dat diezelfde aanpak ook wel eens vruchtbaar zou kunnen worden toegepast ten behoeve van het overbruggen van de kennisasymmetrieën die naar hun aard behoren bij interdisciplinaire samenwerking. Iets voor nader onderzoek, lijkt me.

10 Tenslotte

Waarin wordt afgerond

Ik rond af. Voor het formuleren van effectieve juridische instrumenten die waken tegen het uitbreken van een Cyberpestepidemie is aanmerkelijk meer nodig dan de reflexmatige reactie zoals die in ons huidige politieke klimaat zou kunnen opkomen en die zou aandringen op een direct wettelijk verbod om *agents* die nalaten *bounds checks* uit te voeren in het verkeer te brengen. Zo'n verbod zou hetzelfde gezag kunnen hebben als een wettelijk voorschrift om je oog geopend te houden als de dokter er een medicijn in prutst (ontleend aan [Millikan(2004)]).

Een rechtsorde kent ook reflexen die zich weinig *kunnen* aantrekken van bepaalde regels. Het formuleren van voorschriften kent nu eenmaal valkuilen van alle mogelijke aard. Kennis daarover bestaat in alle mogelijke disciplines. Voor zover de valkuilen zijn onderzocht en beschreven vanuit andere disciplines kan en moet met die kennis rekening worden gehouden, ook door een rechtswetenschappelijke bril. Ik acht de vraag naar welke resultaten dat zijn en hoe er mee te rekenen een belangrijke vraag en neem mij niet alleen voor daar verder onderzoek naar te doen maar ook om de bevindingen ervan over te dragen in het keuzevak Cyberspace en Cyberlaw zolang ik het mag blijven geven. Zoals de rups een cocon spint voor

het gevleugelde wezen dat hij nooit zag maar desalniettemin worden zal, zo spint de rechtswetenschap *regelstelsels* voor een maatschappelijke orde die *zij* nooit zag maar desniettemin mede voortbrengt en bewonen moet. Het ware wenselijk dat dit goed geïnformeerd gebeurde, met de kennis van nu. Ook wanneer die orde een kritische verandering doormaakt.

Noten

[1]**Een korte toelichting op mijn gebruik van eindnoten.**

Ze geven in zekere zin weer hoe het college tot stand is gekomen en bevatten (naast hier en daar een losse referentie) enkele beschouwingen die de bij het ontstaan een rol hebben gespeeld maar de voordracht zelf niet hebben gehaald. Ik neem ze deels op omdat ze achtergrondinformatie bevatten die voor de geïnteresseerde lezer betekenis kunnen hebben, en deels omdat ze de wordingsgeschiedenis laten zien. Ik ben kennelijk begonnen te schrijven voor mezelf en vanuit de abstractie, om orde te kunnen scheppen in mijn woelige gedachtenwereld. Die benadering heeft er – oog in oog met het vereiste een begrijpelijk verhaal te moeten vertellen – toe geleid dat veel van de onderbouwing uiteindelijk in de noten terecht is gekomen.

[2]**De vergelijking.**

Ik heb geen toegang tot de bron van deze vergelijking zoals die door Jones [Jones(1962)] wordt gegeven: Oliver Wendell Holmes Jr., *Collected Papers*, 1920. Jones gebruikte het als verzachtend sluitstuk voor een pessimistische analyse over welke bestemming van de menselijke soort we mogen verwachten in een context waarin we alleen het internationale recht hebben om de immense risico's van de nucleaire tijd tegemoet te treden. Het citaat is geliefd. Bobbitt [Bobbitt(1982)] gebruikte het in aangepaste vorm om de keus van de titel van zijn boek toe te lichten en zelf heb ik het minstens twee keer gebruikt in andere stukken.

[3]**Teleologisch redeneren.**

Zie [Wright(1972), Wright(1973)]. Wright legt in die stukken de ba-

sis voor een formele behandeling van teleologisch redeneren zoals dat bruikbaar kan zijn voor evolutionair georiënteerde wetenschapsbeoefening. Hij geeft daarmee houvast aan die vormen van wetenschapsbeoefening die niet goed uit de voeten kunnen met de domeinbeperkingen die bijvoorbeeld predicatenlogica's van de eerste orde met zich meebrengen. Een fascinerend voorbeeld van de toepasisng ervan acht ik de redeneerwijzen die – ook zonder dat bewust naar Wright wordt gerefereerd – door Sterelny worden gehanteerd in zijn [Sterelny(2006)].

[4] Twee vliegen in één klap.

Nadenkend over hoe dit college aan te pakken heb ik even overwogen dat het efficiënt zou zijn om twee vliegen in één klap te slaan en het voorliggende betoog te benutten als oefening voor het openingscollege van het vak Cyberspace & Cyberlaw in april. Nu geef ik dat vak al jaren. U zou zich dan ook kunnen afvragen waarom het eerste college van dat vak zou moeten worden geoefend. Ik zal proberen dat uit te leggen aan de hand van de titel. Die is me ingegeven door onze inmiddels demissionaire minster-president. Hij heeft de woorden van de titel vleugels gegeven op 12 januari bij zijn bespreking van het rapport van de commissie Davids. De titel luidt: "Met de kennis van nu." (Dinsdag 12 januari 2010, 21:40: Brief kabinet aan 2e kamer. "Met de kennis van nu aanvaardt het kabinet dat voor een dergelijk optreden een adequater volkenrechtelijk mandaat nodig zou zijn geweest"). Ook de president van de Nederlandse bank (Wellink op 1 februari: "met de kennis van morgen" Commissie De Wit) en de oud-voorzitter van de raad van bestuur van ABN-AMRO (Rijkman Groenink op 3 februari: "met de kennis van toen" Commissie De Wit) hebben aan de rijkdom van die titel bijgedragen door oog in oog met de Commissie De Wit erop te variëren: "Met de kennis van nu" krijgt dan mede betekenis in samenhang met formu-

leringen als “met de kennis van morgen” en “met de kennis van toen.” Ik moet u intussen bekennen dat de persconferentie van onze minister-president me beroepsmatig onder de gordel heeft getroffen. Dat is gek, omdat mijn vakgebied, recht en informatica, weinig van doen lijkt te hebben met de volkenrechtelijke beoordeling van een politieke stellingname, anno 2002, over de oorlog met Irak. Wie dat denkt heeft gelijk *en* ongelijk. Gelijk omdat het volkenrecht in dit specifieke geval over oorlog gaat, en niet over informatica. Ongelijk, omdat beide, het volkenrecht en het vakgebied ‘recht en informatica’ tot de rechtswetenschap behoren. En wanneer onze minister-president – een vroegere collega nota bene – rechtswetenschappelijke kennis van nu over een handelen van toen droogjes afserveert als “ook maar een mening” (Dinsdag 12 januari 2010, 10:20: Davids overhandigt rapport Irak aan Balkenende. Een conclusie: volkenrechtelijk mandaat voor de oorlog met Irak ontbrak. Dinsdag 12 januari 2010, 16:30: Persconferentie Balkenende. Conclusie van de commissie over volkenrechtelijk mandaat is “ook maar een mening.”) bekruipt me het onaangename gevoel dat niet alleen onze politieke mores in verval beginnen te raken, maar ook dat de rechtswetenschap er niet best voorstaat. Dat laatste nu trek ik me persoonlijk aan. Eén en ander betekent dat ik in dit college twee dingen wil overbrengen. Het eerste gaat over wat de inhoud zal zijn van het vak Cyberspace en Cyberlaw zoals ik dat in april ga geven. Hiermee grijp ik de gelegenheid aan om u een inkijkje te geven in wat mij vroeger, nu en in de toekomst qua onderzoek interesseert en beweegt. Het tweede gaat over de vraag of, en zo ja hoe die inhoud rechtswetenschappelijk gezag kan claimen dat uitstijgt boven het niveau van “ook maar een mening.”

[5]Een voorbeeld uit de werkelijkheid

Misschien is het goed om bij wijze van terzijde en vooral voor wie niet

gelooft dat het voorbeeld technisch mogelijk is een bericht uit de pers te releveren. In het CNET NEWS van 7 februari 2010 staat een verslag over een stukje demonstratiecode, geschreven door Tyler Shields. Daarmee kan hij naar een Blackberry van iemand anders een SMS sturen die er voor zorgt dat de opgeslagen lijst met namen en nummers per e-mail naar hem wordt verstuurd. Ook kan hij SMSjes sturen die andere functies van de ontvangende Blackberry activeren, zoals het aanzetten van de microfoon en het doorsturen van het aldus verkregen audiomateriaal. Ik leid hieruit af dat de geschetste activiteiten – met de kennis van nu – tot de feitelijke mogelijkheden behoren en dat die mogelijkheden er (om een voorbeeld te noemen) in 2008, ook al waren, zodat de kwetsbaarheid van Obama's Blackberry ook toen al bestond. Alleen was daarover nog niet gepubliceerd. Misschien bestond het vermoeden van de mogelijkheden al wel. Ongeveer het eerste dat hem na de verkiezingen overkwam was dat zijn geliefde Blackberry om veiligheidsredenen werd afgenomen om later te worden vervangen door een bijzonder beveiligd exemplaar.

[6]Enkele definities (Cyberspace, cyberlaw, virtuele werelden, de rechtswetenschap als bril)

Enkele definities (daarbij een *caveat*: mijn definities van 'Cyberspace' en van 'virtuele werelden' wijken af van de gebruikelijke).

Ik roep nog even het wonderlijke telefoongesprek van zo even in herinnering, en de mechanische stem die zegt dat ik een 1 moet toetsen. Waar het me om gaat is om te laten zien dat we in onze relatie tot Cyberspace heel dikwijls in een situatie kunnen geraken waarbij we ons niet kunnen verschuilen achter een afzijdige houding. U toetst de 1 of u doet dat niet. Andere mogelijkheden zijn er niet en beide hebben gevolgen. U bent via Cyberspace in een positie gebracht die doet denken aan wat schakers zetdwang noemen.

Maar wat *is* Cyberspace? De term is een beetje modieus, en ontleend aan de science-fiction literatuur. De term is ingeburgerd als een betrekkelijk vage aanduiding voor wat we als een door de ICT in het leven geroepen virtuele wereld zijn gaan zien. Misschien kan ik met het vreemde telefoontje aangeven wat ik onder Cyberspace versta. Dit is mijn definitie:

Cyberspace is het fysieke gebied waartoe de randapparaten van computers toegang bieden aan personen.

In mijn mobiele telefoon zit een computertje. Misschien zitten er wel meerdere computerjes in. Het uitwendige van mijn telefoon is een *randapparaat* van die computerjes, met het toetsenbordje, het luidsprekertje en de microfoon. Dat randapparaat biedt toegang tot Cyberspace. Wat wij ons bij Cyberspace verder voorstellen is afhankelijk van onze kennis. Als ik mobiel gebeld wordt door mijn zoon uit Wenen, dan verbeeld ik me een radioverbinding van mijn telefoon naar de dichtstbijzijnde GSM-mast, een vaste lijnverbinding die via meerdere schakelpunten een verbinding legt naar Amsterdam, en van Amsterdam via Duitsland naar Wenen, naar de GSM-zendmast die zich het dichtst bij de mobiele telefoon van mij zoon bevindt en tenslotte een radioverbinding naar zijn mobiele telefoon. Intussen zijn meerdere computers aan het werk. Om een telefoonrekening te kunnen sturen registreert mijn telefoonaanbieder wanneer het telefoongesprek begint, van waar naar waar, wanneer het eindigt, en wanneer het door een andere aanbieder wordt doorgeleid, want de Nederlandse en de Duitse en de Oostenrijkse aanbieders die als bemiddelaars van het gesprek optreden moeten ook worden betaald. Wanneer ik mobiel bel met Wenen heb ik zo een aardig zij het nog lang niet volledig functioneel beeld van dat deel van Cyberspace dat nodig is om het gesprek te kunnen voeren. Bij eenvoudige telefonie is Cyberspace in mijn verbeelding een wereldwijd gebied dat bestaat uit een

enorm en complex netwerk van computers en computertjes, verbonden via vaste- en radioverbindingen voor de broodnodige communicatie en voorzien van de juiste programmatuur. Die computers en computertjes handelen autonoom binnen de ruimte die hun daartoe door hun programmatuur wordt geboden. Die autonoom handelende computertjes zijn de actoren die Cyberspace bevolken. Ik noem ze verder *agenten*. Ze moeten positiefrechtelijk goed worden onderscheiden van personen en rechtspersonen: agenten zijn machientjes, het zijn wel actoren, maar ze hebben geen persoonlijkheidsrechten, geen familierechten noch vermogensrechten in de zin van het Nederlands recht. Onder actoren versta ik dus dingen of personen die iets doen. Als de dingen die iets doen computertjes zijn noem ik ze agenten. Ik gebruik de term agent dus niet in de juridisch-technische betekenis van het woord.

Terug naar Cyberspace als fysieke wereld. Hoe kan een mobiele telefoon vanuit Wenen mijn mobiele telefoon in Leiden vinden? Of in Praag, als ik toevallig in Praag ben? Als mijn telefoon aan staat, zoekt die automatisch verbinding met de dichtstbijzijnde GSM-zendmast. Mijn telefoon moet een uniek identificatienummer hebben, net als de telefoon in Wenen. En ergens onderweg moeten zich agenten bevinden die desgevraagd aan andere agenten vertellen waar welke telefoon zich bevindt en van wie die telefoons zijn. En langs welk pad de communicatie het best kan verlopen gegeven de belasting van het net. En die dus moeten weten *hoe* dat moet. In het deel van Cyberspace dat voor mijn telefoongesprekken zorgt werken agenten samen in netwerken. Om dat te kunnen doen moeten ze elkaars taal verstaan en een aantal kunstjes beheersen die het gewenste resultaat opleveren. Het deel van Cyberspace dat voor mijn telefoongesprekken zorgt speelt een communicatiespel met een eigen taal en met eigen regels. Het is mijn stelling dat de agenten in Cyberspace die de mobiele telefonie afhandelen aan één of meer regelstelsels gehoorzamen.

En daarmee zijn we bij mijn tweede definitie die over de regelstelsels in Cyberspace gaat, over Cyberlaw dus. Die luidt als volgt:

Cyberlaw is de verzameling van regelstelsels die in jurisdicties binnen Cyberspace gelden voor de agenten die binnen die jurisdictie vallen.

Cyberspace onderscheidt zich in mijn definitie uitdrukkelijk van wat 'de virtuele wereld' wordt genoemd. *Die* definieer ik als volgt:

De virtuele wereld is wat onze verbeelding bewerkstelligt, in interactie met dat wat de randapparatuur van Cyberspace ons presenteert.

De virtuele wereld is in mijn opvatting sterk verwant aan de wereld die door een toneelvoorstelling wordt opgeroepen bij de toeschouwer: alleen wordt de voorstelling nu gepresenteerd door randapparatuur en verzorgd door de onzichtbare agenten in Cyberspace. Het voorbeeld van een virtuele wereld is wat uw verbeelding u voorspiegelt wanneer u naar een beeldscherm kijkt en deelneemt aan een computerspel of aan wat Second Life u laten zien.

Tenslotte: om Cyberspace, Cyberlaw en de virtuele wereld binnen het domein van de rechtswetenschap te kunnen plaatsen omhels ik de hypothese van de rechtswetenschap als bril. Ook daarvan heb ik een definitie:

Wie de rechtswetenschap als bril gebruikt meent dat het zin heeft om alle gemeenschappen van actoren volgens de elementaire karakteristieken van regelgeleide gemeenschappen te analyseren.

Deze hypothese ligt aan de basis van het inzicht dat het recht zich heeft mee-ontwikkeld met onze evolutie, en dat die afkomst kan worden herkend aan de structurele verwantschap in de 'rechtsordes' van alle mo-

gelijke gemeenschappen van actoren, niet alleen van natiestaten en verdragsorganisaties, maar ook van gezinnen, bedrijven, overheidsdiensten, markten en voetbalclubs. Met de rechtswetenschap als bril proberen we die instituties te begrijpen in termen van – bijvoorbeeld – orde, regels, sancties, gebruiken, taken en discretionaire bevoegdheden. Door deze bril kunnen we zelfs proberen gemeenschappen van chimpansees of bijen te begrijpen en te beschrijven met als doel te achterhalen of we daar weer iets van zouden kunnen leren voor onze eigen rechtsgemeenschappen. Door diezelfde bril kunnen we proberen te kijken naar gemeenschappen van agenten, van zelfstandig werkende computerprogrammaatjes. Mijn stelling is dat het zin kan hebben een structurele verwantschap te zien tussen traditionele rechtsordes en de ordes in gemeenschappen van samenwerkende agenten in Cyberspace. Meer over mijn benadering van insituties in [Schmidt(2009)].

Ik geef een vergelijking ter nadere toelichting. Stelt u zich een flipperkast voor in een Nederlandse horecagelegenheid, een flipperkast met twee knoppen waarmee u de flippers kunt besturen om de bal in het spel te houden die, zolang die in het spel is op ruwe wijze door wat ik nu maar even "bumpers" noem wordt rondgeschoten. Ik geef een paar kanttekeningen via deze flipperkastmetafoor.

- Allereerst: U staat in een Nederlandse horecagelegenheid: voor u en uw gedrag in de fysieke wereld geldt het Nederlands recht.
- Ten tweede: er is nog een wereld die zich ontwikkelt tijdens uw interactie met de flipperkast. Dat is de wereld die uw verbeelding schept als ware u gewikkeld in een spel. Daar ziet u de bal bewegen en ziet u ook de resultaten van wat u met de flippers uitvoert en daar ziet u hoeveel punten u bij elkaar heeft gespeeld en of u een vrij spel heeft verdiend. Dat is de virtuele wereld. Deze

wereld heeft een eigen rechtsorde. In deze wereld gelden, naast of in aanvulling op het Nederlandse recht de al dan niet op de verkeersopvatting rustende verplichtingen die bij het spel behoren. Mijn stelling is dat het merendeel van de vraagstukken uit het informatierecht hier spelen. Zomin het vanzelfsprekend is dat een gestrekt been in de virtuele wereld van het voetbalspel als poging tot zware mishandeling wordt gezien, zomin is het vanzelfsprekend dat het dwingende Nederlandse recht onverkort geldt in de virtuele werelden van mijn definitie. Rechtswetenschappelijke vragen over virtuele werelden zijn fascinerend en maatschappelijk belangrijk, maar ze vormen niet het hoofdonderwerp van dit college – daarvoor moet u bij onze andere vakken zijn.

- Ten derde: onder het speelveld van de flipperkast, onzichtbaar voor de speler, bevindt zich een gemengd mechanische, elektronische en elektromagnetische wereld met relais, en computertjes, met de onzichtbare kant van de bumpers, verbonden door communicatiedraden. Die fysieke wereld, die u vanuit uw positie helemaal niet te zien krijgt, is vergelijkbaar met wat ik Cyberspace noem, met onder meer de bumpers als agenten. Ook deze wereld heeft zijn eigen 'rechtsorde.' De regels die in deze wereld gelden bepalen het gedrag van de bumpers, en daarmee in belangrijke mate het gedrag van de "pin-ball."

- Ten vierde: bestaan en ontstaan van Cyberspace vloeien voort uit menselijk handelen. Ze zijn ontworpen en tot stand gebracht, en worden beschikbaar gesteld met een doel, onder verantwoordelijkheid van personen die onder de jurisdictie van het traditionele recht vallen. Ook tussen makers, aanbieders en gebruikers van agenten in Cyberspace kan een rechtsorde worden gezien. Eén van de redenen om afzonderlijk rechtswetenschappelijke aandacht

te vragen voor Cyberlaw ligt in de omstandigheid dat wat ik eerder het verantwoordelijkheidslek heb genoemd zich in toenemende mate laat zien en voortvloeit uit tekortkomingen in deze rechtsorde.

[7]**Het Hart-Fuller debat**

Zie: [Hart(1957)] en [Fuller(1957)].

[8]**Inbreng, relevant voor de rechtswetenschap die door de passende lens omziet naar kritische veranderingen in de maatschappelijke orde (een bloemlezing):**

- Montesquieu [Montesquieu(1748)],
- Smith [Smith(1776)],
- Darwin [Darwin(1859)],
- Coase [Coase(1937)],
- Von Neumann [von Neumann(1945)],
- Popper [Popper(1945)],
- Simon [McGuire and Radner(1972)],
- Cohen [Cohen(1972)],
- Fuller [Fuller(1978)],
- Dijkstra [Dijkstra(1979)],
- Hofstadter [Hofstadter(1979)],
- Hoare [Hoare(1981)],

- Gitlin [Gitlin(1980)],
- Myerson [Myerson(1988)],
- North [North(1990)],
- Douglas [Douglas(1992)], Posner [Posner(1992)],
- Olson [Olson(2000)],
- Hirshleifer [Hirshleifer(2001)],
- Hodgson [Hodgson(2004)],
- Williamson [Williamson(2005)],
- Greif [Greif(2006)],
- Sterelny [Sterelny(2006)],
- Dawkins [Dawkins(2006)],
- De Waal [de Waal(2009)],
- Gintis [Gintis(2009)],
- Scheffer [Scheffer(2009)].

[9]**Een econoom met aandacht voor een onderscheid tussen de morele en de amorele *homo economicus***

Zie:[Hirshleifer(2001)].

[10]**De overheidsmonitor over cybercrime**

Zie: [govcert.nl(2009)].

[11]**Het Sneker Botnet in de pers**

Uit WebWereld (http://webwereld.nl/nieuws/52382/verkoop-sneker-botnet-was–ripdeal-.html)

“Gepubliceerd: Donderdag 21 augustus 2008 Auteur: Jan Libbenga

De 19-jarige Sneker die onlangs werd opgepakt omdat hij voor 25.000 euro een botnet aan een Braziliaan wilde verkopen, blijkt helemaal niet de eigenaar van dat botnet te zijn.

Dat vertellen gebruikers van het botnet aan Webwereld.

Noredin Nasiri, op het web beter bekend als Woopie en werkzaam bij een datacenter, werd onlangs opgepakt door het Het Team High Tech Crime van de Nationale Recherche na een tip van de FBI.

Het OM ging ervan uit dat de 19-jarige man uit Sneek over een botnet van ongeveer 100.000 geïnfecteerde computers zou beschikken. Een botnet of robotnetwerk is een groep van geïnfecteerde computers, die op afstand vanuit een centraal punt worden gemanipuleerd. Botnets worden door criminelen gebruikt om op grote schaal spam te versturen, creditcard- of bankgegevens te onderscheppen of denial of service aanvallen op websites uit te voeren.

Het Korps Landelijke Politiediensten greep in toen N. het botnet wilde verkopen aan een 35-jarige Braziliaan die het net voor criminele activiteiten wilde inzetten. De Braziliaan is ook opgepakt en wordt uitgeleverd aan de Verenigde Staten.

Bronnen vertellen Webwereld dat de Sneker helemaal geen eigenaar is van het botnet: het is eigendom van een Rus. Het netwerk wordt onder meer gebruikt voor honeypot-achtige activiteiten: het dient als lokaas om criminelen binnen te halen en te identificeren.

Wellicht heeft het OM geconcludeerd dat N. zelf de beheerder van het botnet was omdat hij de broncode van de benodigde software op zijn computer had staan, zo vermoeden insiders. Maar in feite had hij alleen maar toegangsrechten die hij aan de Braziliaan wilde verkopen. Binnen de wereld van online computercriminaliteit staat dit bekend als een 'ripdeal': een term die geleend is uit de drugswereld waarbij één criminele groep wordt beroofd door de andere, die de buit vervolgens doorverkoopt.

De Russische eigenaar weet pas sinds kort van het incident en was dan niet op de hoogte van de verkoop-actie. Het netwerk is inmiddels weer in gebruik genomen.

De KLPD wilde niet ingaan op vragen van Webwereld zolang het onderzoek nog gaande is."

[12]**Hoare's Turing Award Lecture uit 1980**

Zie [Hoare(1981)].

[13]**Lapmiddelen**

Ik noem drie maatregelen die beogen om ook in situaties waarin bounds checks worden nagelaten soulaas te bieden. Het zijn lapmiddelen:

- Een ervan heet *address space layout randomization* (ook wel: ASLR) en zorgt ervoor dat functies niet meer worden gerelateerd aan vaste geheugenadressen, maar dat hun geheugenlocatie bij het laden wordt gerandomiseerd. De gedachte is dat wie misbruik maakt van een *buffer overflow vulnerability* om de program counter aan te passen en niet weet waar de program counter staat vermoedelijk een crash van het betreffende programma/systeem veroorzaakt in

plaats van de controle ervan over te nemen. ASLR beschermt ons weliswaar vergaand tegen het misbruik maken van buffer overflow vulnerabilities, maar leidt bij succes tot crashes. Vanuit het gezichtspunt van de gebruiker niet een remedie tegen, maar óók een symptoom van de Cyberpest.

- De tweede maatregel is een aanvulling op ASLR. Misbruikers kunnen systematisch via herhaling proberen te gissen waar de program counter is opgeslagen (en daarbij reeksen van systeem- of programmacrashes veroorzaken). Om die reden is een aanvullende voorziening nodig die de regelmaat waarmee dergelijke crashes voorkomen analyseert en maatregelen treft wanneer ze systematisch worden veroorzaakt. Hiermee kan aannemelijk worden gemaakt *dat* er een *vulnerability* wordt aangevallen.

- Om nader te kunnen onderzoeken *welke* vulnerability wordt aangevallen is nog een aanvullende maatregel nodig: *logging*. Logging houdt in dat de computer in kwestie *zijn* gedrag – en dat de agenten die erop draaien *hun* gedrag – registreren, bewaren en beschikbaar houden voor onderzoek naar welke vijandige agenten misbruik maken of proberen te maken en van welke *vulnerability*.

Het slagveld overziend lijkt het met de kennis van nu niet goed mogelijk om een aanval van Cyberpest in de kiem te smoren. Het op grote schaal veronachtzamen van *bounds checking* in systeemprogrammatuur en in gebruiksprogrammatuur waarvan we inmiddels allemaal afhankelijk zijn geworden is daarvan de oorzaak. En de thans in zwang komende lapmiddelen als *address space randomization* en *logging* veranderen de pijn in zoverre, dat onze computers niet onder commando van kwaadwillenden komen, maar crashen. Computers die crashen in opdracht van een kwaadwillende buitenstaander zijn ook symptomen van de Cyberpest.

[14]De rechtswetenschap heeft een trifocale bril

Laat ik aangeven wat ik onder "wat rechtens is" versta en op welke manieren ik meen dat de rechtswetenschap aan het rationeel beoordelen van wat rechtens is en wat rechtens zou moeten zijn pleegt bij te dragen. De achterliggende gedachte is dat wanneer we dat voor gemeenschappen van personen weten, we een aanknopingspunt hebben om over wat rechtens is in gemeenschappen van agenten in Cyberspace na te denken. Een belemmering is dat de gemeenschap van rechtswetenschapbeoefenaren verdeeld is als het over de vraag gaat wat rechtswetenschap nu eigenlijk is.

Gelukkig is de rechtswetenschap meerdere millennia oud en even gelukkig heeft zich daarbinnen een specialisatie ontwikkeld die over de vraag naar "wat rechtens is" op theoretisch niveau nadenkt en debat voert. In dat debat zijn drie hoofdstromen waarvan ik meen dat elk zich tegenover de andere twee al tenminste enkele eeuwen weet te handhaven. Ik doel op het rechtsrealisme, op het rechtspositivisme en op het rechtsnaturalisme. Ik meen dat ze elkaar geenszins uitsluiten, maar dat elk van de drie stromingen zijn eigen functie heeft naast de twee andere. Om te laten zien hoe dat werkt gebruik ik de ontvangst van het rapport Davids weer even als illustratie.

1. Vanuit realistisch perspectief is "wat rechtens is" af te lezen uit wat rechters, advocaten, het Openbaar Ministerie met en voor rechtzoekenden ten aanzien van concrete situaties in feite doen. In deze visie is dat wat rechtens is gelijk aan de rechtspraktijk. Het realistische perspectief is dus beschrijvend en de wetenschappelijke kwaliteit ervan afhankelijk van nauwkeurige waarneming en onafhankelijke analyse. Davids hanteerde het realistische perspectief bij het beschrijven van de gang van zaken in het kabinet in 2002.

Wetenschappelijk valt daar niets op aan te merken. Die beschrijving is niet "ook maar een mening," maar feitenkennis. Wetenschapspopulistisch geldt hier het adagium: "feiten zijn feiten."

Het realistische perspectief heeft verschillende onmisbare *functies* in rechtswetenschappelijke beschouwingen. Eén functie is om te laten zien wat de (rechts)praktijk is. Wetenschappelijk hebben we dat gezichtspunt en de bijbehorende kennis nodig om de rechtspraktijk aan de hand van criteria te kunnen beoordelen. Zonder realistisch beeld van de rechtspraktijk is een normatief oordeel over de rechtspraktijk onmogelijk. Davids kan niets juridisch zeggen over de gang van zaken in het kabinet rond Irak, zonder een realistisch beeld van die gang van zaken, zoals ons kabinet in 2002 niets volkenrechtelijks kan zeggen over de gang van zaken in Irak zonder een realistisch beeld over de vraag of Irak daadwerkelijk binnen 45 minuten massavernietigingswapens kon inzetten. Maar er is nog een tweede aspect: zonder realistisch beeld van de rechtspraktijk is het onmogelijk om eraan bij te dragen dat de rechtspraktijk als geheel coherent *blijft*, ook als deze zich ontwikkelt. Het rechtsrealisme treedt niet in plaats van het positivisme of het naturalisme, het biedt er het onmisbare fundament voor.

Het hier geschetste beeld is geïnspireerd op de presentatie ervan door Oliver Wendell Holmes jr.[Wendell Holmes Jr(1897)] uit 1897. Zijn stelling dat de invloed van het recht op het gedrag van rechtssubjecten vooral berust op hun ervaringen met de rechtspraktijk heeft hem bij de rechtsfilosofen weinig populair gemaakt, ook al lijkt die stelling me na meer dan honderd jaar nog steeds goed verdedigbaar. Ik ga nu over naar het volgende gezichtspunt.

2. Vanuit positivistisch perspectief is "wat rechtens is" af te lezen uit het geldende recht. De positivistische rechtswetenschap legt

de nadruk op hoe het geldende recht moet worden gelezen in het licht van een voorgelegde situatie. Het positivistische perspectief is dubbel normatief: ten eerste omdat het ervan uitgaat dat het formeel geldende recht de inhoudelijke norm stelt en ten tweede omdat de rechtswetenschap de normatieve eisen stelt over hoe het positieve recht moet worden gelezen. Davids hanteerde het positivistische perspectief bij zijn vaststelling dat een toereikend volkenrechtelijk mandaat voor de oorlog met Irak ontbrak. Wetenschappelijk valt daar niets op aan te merken. Uitgaande van het destijds geldende volkenrecht en van de destijds rechtswetenschappelijk geldende interpretatiemethoden is die vaststelling niet "ook maar een mening," maar rechtswetenschappelijke kennis, gebaseerd op de ordentelijke interpretatie van de regels. Wetenschapspopulistisch is de slogan hier "regels zijn regels."

Het positivistische perspectief heeft eveneens een onmisbare functie voor rechtswetenschappelijke beschouwingen. Het geeft ons de betekenis van de wet als toepasselijk op concrete situaties, door na te gaan of de wet volgens geldige procedures tot stand is gekomen en door een beperkt repertoire aan interpretatiemethoden toe te passen. Uit die aanpak vloeit rechtszekerheid voort. Het positivistische perspectief beschermt naar zijn aard de juridische *status quo* en komt dan ook het beste tot zijn recht in situaties waarin die er is en overeenkomt met het heersende rechtsgevoel. In een stabiele rechtsorde dus.

In hun beroemde controverse plaatsten Hart (o.c.) en Fuller (o.c.) het positivisme en het naturalisme diametraal tegenover elkaar. Ik denk dat dat niet hoeft waar, anders dan het positivisme, het naturalisme vooral tot zijn recht komt waar de rechtsorde instabiel is of dreigt te worden.

3. Vanuit naturalistisch perspectief is “wat rechtens is” gelijk aan “wat rechtens zou moeten zijn.” Het wordt heel vaak op een niet-wetenschappelijke manier, dat wil zeggen: op een ongefundeerde en/of oncontroleerbare manier gehanteerd – als ware “dat wat rechtens zou moeten zijn” vanzelfsprekend gegeven, bijvoorbeeld door een innerlijk stem, door God of door de “natuur der dingen.” Het naturalistisch perspectief klinkt luid door in de opvatting van Van Walsum dat het regeringen onder omstandigheden vrij staat van het volkenrecht af te wijken. Rechtswetenschappelijk gezien zijn het de redeneringen die een beroep doen op het natuurrecht die het dichtst komen bij wat kan worden afgeserveerd als “ook maar een mening.”

   Het wordt steevast van stal gehaald wanneer een rechtsorde in zich bedreigd weet, van binnenuit of van buiten. Daarmee is het naturalistische perspectief verontrustend. Het wordt vaak als legitimatie gebruikt voor eigenrichting, politieke moorden, culturele revoluties en terroristische activiteiten. Maar het is ook als legitimatie gebruikt voor ons Plakkaat van Verlatinghe van 1581, voor de Franse revolutie, voor het verzet in de tweede Wereldoorlog, voor de Praagse Lente en voor het openen van de Chinese deuren. Met andere woorden, het naturalistisch perspectief is scherp aan beide kanten. En het is het belangrijkste werktuig van populisten, die goed op gevaren kunnen wijzen maar hun remedies niet onderbouwen.

   Wetenschapspopulistisch is de slogan die bij de natuurrechtelijke provincie hoort *“Ordnung muß sein.”* Die slogan brengt de aanname tot uitdrukking dat er onafwendbare, natuurlijke en universele krachten zijn die tot het ontstaan van orde in gemeenschappen aandringen. (Coase schetste die kracht in 1937 vanuit

economisch perspectief [Coase(1937)]; hij kan ook heel goed worden herkend in de onzichtbare hand van Smith [Smith(1776)] en in de evolutietheorie van Darwin [Darwin(1859)]). Die krachten kunnen in conflict komen met de door mensenhand ontworpen orde die doorklinkt in het positieve recht. Dat kan leiden tot de zojuist genoemde 'natuurrechtverschijnselen.'

Ik merk ook op dat de rechtswetenschap daar nauwelijks aandacht voor heeft. Dat kan goed worden verdedigd vanuit de gedachte dat die aandacht in de sociale wetenschappen meer voor de hand ligt en dat de verdeling van onderwerpen over de verschillende disciplines er niet voor niets is. Minder vanzelfsprekend vind ik het daarentegen dat de rechtswetenschap niet of nauwelijks aandacht heeft voor de rollen die het recht en de rechtswetenschap *zelf* spelen, als onderdeel van c.q. mede-oorzaak voor bedoelde natuurrechtverschijnselen. Ik kom hier op terug.

Ik vat samen. De rechtswetenschap kent drie benaderingen die respectievelijk kunnen worden getypeerd met 'feiten zijn feiten,' 'regels zijn regels' en '*Ordnung muß sein.*' Voor die laatste benadering is weinig empirische rechtswetenschappelijke belangstelling: we weten er dus weinig van.

[15]**Beperking in de gesproken tekst**

Ik laat in de gesproken tekst het rechtsrealisme weg – dat is impliciet inmiddels voldoende aan de orde geweest.

[16]**Voor een gegeneraliseerde beschouwing over 'critical transitions'**

Zie: [Scheffer(2009)].

[17]**Een wetenschappelijk fundament onder bestuurlijke maakbaarheid en zijn beperkingen**

Zie ook Van Gunsteren in [Van Gunsteren(1976)].

[18]**Drie additionele bevindingen uit de informatica**

Pas in de jaren 70 van de vorige eeuw werden computers op meer dan incidentele schaal buiten de wetenschap ingezet voor andere dan defensiedoeleinden: voor administratieve processen bij banken en verzekeraars bijvoorbeeld. Dit leidde onmiddellijk tot een crisis die de software-crisis werd genoemd: wat informatici dachten te kunnen maken mislukte in de praktijk zeer regelmatig en spectaculair. Rond 1975 heeft deze universiteit, bijvoorbeeld, zijn hele personele en financiële administratie in één informatiesysteem willen onderbrengen. Dat project bleef zonder resultaat en heeft de universiteit destijds 20 miljoen guldens gekost. Dijkstra en Hoare hebben een weg gewezen om de software crisis het hoofd te bieden. Hun aanbevelingen zijn informatica-technisch van aard en gaan onder meer over het gebruik van *pointers, goto statements* en bounds *checks*. Ik vat hun inzichten samen met behulp van een door Dijkstra zelf verafschuwde term die desalniettemin is ingeburgerd. Zie bijvoorbeeld [Dijkstra(1979)] en [Dahl et al.(1972)Dahl, Dijkstra and Hoare].

Deze bevinding zou verder kunnen worden aangevuld met (1) het vereiste om bij de inrichting van databases gebruik te maken van het werk van Codd (het relationele datamodel voor de structurering van databases en SQL voor bevragen en bewerken ervan), en (2) het vereiste dat de methoden van requirements engineering moeten worden gebruikt bij de ontwikkeling van programmatuur. Zie bijvoorbeeld [Wieringa(1997)] en/of [Schreiber et al.(2000)], en (3) het vereiste dat bij het gebruik van hulpmiddelen als C++ en de object georiënteerde modelleermethoden, de

vereisten van stuctured programming niet moeten losgelaten, ook niet wanneer die hulpmiddelen daartoe uitnodigen. Deze bevinding is controversieel en daarmee alleen van theoretische betekenis. (De vraag naar efficiënte en functioneel betrouwbare programmatuur was destijds veel groter dan het aanbod. Mede onder die druk kwamen nieuwe programmeertalen en ontwerpmethoden als C en C++ beschikbaar, talen waarin de *bounds check* optie zelden werd aangezet en waarin het meest gruwelijke gebruik van pointers mogelijk was – iets waarvan veelvuldig gebruik werd gemaakt om programmatuur zo snel mogelijk te kunnen maken en te laten werken. Ook de nieuwe standaard voor ontwikkelen van programmatuur volgens object georiënteerde methoden is toen ingeburgerd geraakt, een methode waarbij veel van de zekerheden van Codd's relationele datamodel weer werden prijsgegeven. Zie bijvoorbeeld: [Grady Booch and Jacobson(1998)] en [Ambler(2003)]).

[19]**Kennisasymmetrie en ad-hoc transacties**

Zie bijvoorbeeld: [Akerlof(1970)].

[20]**Kennisasymmetrie en duurcontracten**

Zie bijvoorbeeld: [Williamson(2005)].

[21]**Over de ontwikkeling van economieën en de rol van padafhankelijkheid, bijvoorbeeld**

Zie bijvoorbeeld [North(1990)].

[22]**Twee additionele inzichten uit de sociale wetenschap**

Er zijn nog twee inzichten uit de sociale wetenschappen die de uitgesproken tekst niet hebben gehaald hoewel ze een rol zouden kunnen spelen bij de *effectieve* overdracht en bekendmaking van wetenschapsre-

sultaten in de rivchting van beslissers, ook via de media, terwijl mijn bijdrage niet die van een activist is, maar vanuit de (ouderwetse) wetenschapsopvatting waarin publicatie nog van primair- en het genereren van maatschappelijke roering van secundair belang wordt geacht. Het gaat om de volgende.

- Het inzicht dat met de keuze van de bewoording van een stelling een hele emotioneel-politieke context kan worden mee-overgedragen die eventuele tegenstanders al in de verdedigingplaatst nog voordat een discussie is gevoerd. Het inzicht heeft de naam *'framing'* gekregen en wordt onder meer wetenschappelijk verantwoord door Gitlin [Gitlin(1980)]. Juridisch is het vooral van belang in de rechtspraktijk en is het een belangrijk wapen waarmee de ene partij het de ander moeilijk kan maken. Het zou bijvoorbeeld kunnen worden verdedigd te hebben plaatsgevonden bij de eerste veroordeling van Lucia deB., met behulp van statistiek (zie ook de bijdrage van Richard Gill onde de titel Lies, Damned lies and legal thruths in het indrukwekkende boek dat me [Mommers et al.(2010)] werd aangeboden). Ook de term 'Cyberpest' die ik in dit college introduceerde is een vorm van *framing*. Het klassieke voorbeeld is de wijze waarop de uitslag van een wedstrijd tussen twee partijen kan worden gepresenteerd: de winnaar wordt dan eennalaatste.

- Het inzicht dat het om de aandacht te trekken bijzonder effectief is om het beoogde onderwerp te vertalen in een dreigende ramp op grote schaal. De commotie die dat kan oproepen wordt een *'moral panic'* genoemd. Cohen legde er een wetenschappelijke basis onder in zijn [Cohen(1972)]. Het creëren van moral panics is inmiddels van steeds groter praktisch belang geworden in een wereld waar informatie op zo grote schaal beschikbaar is dat een bericht op zijn

eigen 'verdiensten' nauwelijks meer de aandacht kan trekken die het mogelijk verdient. Moral panics roepen in de Westerse wereld een bekend patroon van reacties op dat op alle manieren (bewust en onbewust) wordt gebruikt, zowel in de pers (waar het een belangrijk middel om te overleven is geworden) als in de politiek. Douglas en Wildawski [Douglas and Wildavski(1982)] wijdden aan dat laatste een intrigerend boek, en Smits [Smits(2002)] een boeiend proefschrift. In de strafrechtspraak is men al langer met het verschijnsel vertrouwd en wordt het bij de straftoemeting besproken onder het kopje maatschappelijke beroering of aanverwante termen. Moral panics zijn doorgaans dé wapens van populisten.

[23]**Een externe en een interne coherentievraag**

Een fascinerend vraagstuk is bijvoorbeeld wat de auteursrechthebbende nog te zeggen heeft over de noodzakelijke wijzigingen die aan zijn programma moeten worden aangebracht wanneer een toekomstige lezing van de risicoaansprakelijkheid de gebruiker ervan zou dwingen om *bounds checks* alsnog te realiseren.

Minstens even fascinerend is de juridische problematiek die wordt opgeroepen door kennisasymmetrieën en die bij economen als *moral hazards* in het centrum van de belangstelling staan. Kennisasymmetrieën kunnen niet alleen een markt in gevaar brengen, ze kunnen ook een bijl leggen aan de één van de wortels van de juridische boom van kennis van goed en kwaad: ze dreigen immers de betekenis van het concept 'wilsovereenstemming' te bederven.

[24]**Over aanbesteding en de kennis van nu**

Zie: [Schmidt and Corvers(2009)]

Aangehaalde literatuur

[Akerlof(1970)] Akerlof, G. A., "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics* 84 (1970), 488–500.

[Ambler(2003)] Ambler, S. W., *Agile database techniques: effective strategies for the agile software developer* (John Wiley & Sons, Inc. New York, NY, USA, 2003).

[Bobbitt(1982)] Bobbitt, P., *Constitutional Fate: Theory of the Constitution* (Oxford University Press, 1982).

[Coase(1937)] Coase, R. H., "The Nature of the Firm," *Economica* 4 (November 1937), 386–405.

[Cohen(1972)] Cohen, S., *Folk devils and moral panics* (MacGibbon and Kee, 1972).

[Dahl et al.(1972)Dahl, Dijkstra and Hoare] Dahl, O., E. Dijkstra and C. Hoare, *Structured programming* (Academic press, 1972).

[Darwin(1859)] Darwin, C., *On the Origin of Species by Means of Natural Selection or, The Preservation of Favoured Races in the Struggle for Life* (Collector's Library (2004), 1859).

[Dawkins(2006)] Dawkins, R., *The God Delusion* (Bantam Press, 2006).

[de Waal(2009)] de Waal, F. B. M., "Darwin's last laugh," *Nature* (2009), 175.

[Dijkstra(1979)] DIJKSTRA, E., "Go to statement considered harmful," (1979), 27–33.

[Douglas(1992)] DOUGLAS, M., *Risk and Blame: Essays in Cultural Theory* (Routledge, 1992).

[Douglas and Wildavski(1982)] DOUGLAS, M. AND A. WILDAVSKI, *Risk and Culture: an Essay on the Selection of Technological and Environmental Dangers* (University of California Press, 1982).

[Fuller(1957)] FULLER, L. L., "Positivism and fidelity to law–A reply to Professor Hart," *Harvard Law Review* 71 (1957), 630.

[Fuller(1978)] ———, "The forms and limits of adjudication," *Harvard Law Review* 92 (1978), 353–409.

[Gintis(2009)] GINTIS, H., *The bounds of reason: game theory and the unification of the behavioral sciences* (Princeton University Press, 2009).

[Gitlin(1980)] GITLIN, T., *The Whole World is Watching: Mass Media in the Making and Unmaking of the Left* (Univeristy of California Press, 1980).

[govcert.nl(2009)] GOVCERT.NL, *Trendrapport 2009: Inzicht in cybercrime: trends & cijfers* (govcert.nl, 2009).

[Grady Booch and Jacobson(1998)] GRADY BOOCH, J. R. AND I. JACOBSON, *The Unified Modeling Language User Guide* (Addison-Wesley, 1998).

[Greif(2006)] Greif, A., *Institutions and the Path to the Modern Economy: Lessons from Medieval Trade* (Cambridge University Press, 2006).

[Hart(1957)] Hart, H., "Positivism and the Separation of Law and Morals," *Harvard Law Review* 71 (1957), 593.

[Hirshleifer(2001)] Hirshleifer, J., *The Dark Side of the Force* (New York: Cambridge University Press, 2001).

[Hoare(1981)] Hoare, C., "The Emperor's Old Clothes," *Communications of the ACM* 24 (1981), 75–83.

[Hodgson(2004)] Hodgson, G., "Darwinism, causality and the social sciences," *Journal of Economic Methodology* 11 (2004), 175–194.

[Hofstadter(1979)] Hofstadter, D. R., *Gödel, Escher, Bach: an Eternal Golden Braid* (Basic Books, 1979).

[Jones(1962)] Jones, H., "Law and the Idea of Mankind," *Columbia Law Review* 62 (1962), 753–774.

[McGuire and Radner(1972)] McGuire and Radner, eds., *Decision and Organization*, chapter Theories of Bounded Rationality (North-Holland Publishing Company, 1972), 161–176.

[Millikan(2004)] Millikan, R., *Varieties of Meaning, the 2002 Jean Nicod lectures* (MIT Press, 2004).

[Mommers et al.(2010)] Mommers, L. et al., eds., *Het binnenste buiten - Liber Amicorum ter gelegenheid van het emeritaat*

van prof. dr. Aernout H.J. Schmidt, hoogleraar Recht en Informatica te Leiden (eLaw@Leiden, 2010).

[Montesquieu(1748)] MONTESQUIEU, *De l'Esprit des Lois* (Constitution Society, 1748).

[Myerson(1988)] MYERSON, R., "Incentive constraints and optimal communication systems," in *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge* (Morgan Kaufmann Publishers Inc. San Francisco, CA, USA, 1988), 179–193.

[North(1990)] NORTH, D., *Institutions, Institutional Change and Economic Performance* (Cambridge University Press, 1990).

[Olson(2000)] OLSON, M., *Power and Prosperity: Outgrowing communist and capitalist dictatorships* (Basic Books, 2000).

[Popper(1945)] POPPER, K. R., *The Open Society and its Enemies* (Routledge, 1945).

[Posner(1992)] POSNER, R., "The new institutional economics meets law and economics," *Wettbewerbsrechtliche Schranken für staatliche Massnahmen nach europäischem Gemeinschaftsrecht* (1992), 73.

[Scheffer(2009)] SCHEFFER, M., *Critical transitions in nature and society* (Princeton Univ Pr, 2009).

[Schmidt(2009)] SCHMIDT, A., "Radbruch in Cyberspace: About Law-System Quality and ICT Innovation," *Masaryk Univer-*

sity Journal of Law and Technology (Also available at SSRN: http://ssrn.com/abstract=1423105) (2009).

[Schmidt and Corvers(2009)] Schmidt, A. and S. Corvers, *Aanbesteding en innovatie: juridisch handboek functioneel specificeren van aanbestedingen* (Sdu, 2009).

[Schreiber et al.(2000)] Schreiber, G. et al., *Knowledge Engineering and Management: The CommonKADS Methodology* (MIT press, 2000).

[Smith(1776)] Smith, A., *An Inquiry into the Nature and Causes of the Wealth of Nations* (Project Gutenberg, 1776).

[Smits(2002)] Smits, M., *Monsterbezwering - de culturele domesticatie van nieuwe technologie* (Boom, 2002).

[Sterelny(2006)] Sterelny, K., "Memes revisited," *The British Journal for the Philosophy of Science* 57 (2006), 145.

[Van Gunsteren(1976)] Van Gunsteren, H., *The quest for control: a critique of the rational-central-rule approach in public affairs* (Wiley, 1976).

[von Neumann(1945)] von Neumann, J., "First Draft of a Report on the EDVAC by John von Neumann, Contract No. W-670-ORD-4926, Between the United States Army Ordnance Department and the University of Pennsylvania Moore School of Electrical Engineering University of Pennsylvania June 30, 1945," Technical Report, University of Pennsylvania Moore School of Electrical Engineering, 1945.

[Wendell Holmes Jr(1897)] Wendell Holmes Jr, O., "The Path of Law," *Harvard Law Review* 10 (1897), 457–478.

[Wieringa(1997)] Wieringa, R., *Requirements Engineering: Frameworks for Understanding* (Wiley, 1997).

[Willemsen(1987)] Willemsen, A., *De taal als bril* (De Arbeiderspers, 1987).

[Williamson(2005)] Williamson, O. E., "The Economics of Governance," *American Economic Review* 95 (2005), 1 e,v,.

[Wright(1972)] Wright, L., "Explanation and teleology," *Philosophy of Science* (1972), 204–218.

[Wright(1973)] ———, "Functions," *Philosophical Review* 82 (1973), 139–168.